

Security Awareness Newsletter

Published by the GOT Division of Security Services

July 2003

Volume 1, Issue 4



Inside this issue:

**New McAfee
AVD License
Agreement** 1

**Escaping the Wrath
of Bugbear.B** 1

**Security Alerts:
How They Can
Help Protect Your
Systems** 2

**HELP—I Have a
Virus!** 2

New WLAN Policy 3

Using Email Wisely 3

Cyber Bytes 4

Microsoft Info 5

**Additional Security
Resources** 6

New McAfee Active Virus Defense (AVD) License Agreement

In June, the State's CIO, Aldona Valicenti, announced the new licensing agreement between the Commonwealth of Kentucky and Network Associates, Inc. (NAI) for McAfee anti-virus products. McAfee is the state's enterprise standard for virus protection.



The license agreement this year is structured differently than it has been in the past. GOT will not be purchasing the licenses for agencies and then billing them via the "pass-thru" process. Instead, agencies will work directly with NAI to purchase needed McAfee licenses.

This statewide agreement includes a "consumer home use" option for agencies to purchase to allow employees to install McAfee products on their home computers. GOT strongly recommends the purchase of this option, especially for those agencies who have numerous staff that access the Commonwealth's networks from home.

For more information, see Agency Contact Memo #2003-0601 available in GOTSource at <http://www.gotsource.net/dscgi/ds.py/View/Collection-7184>.

Escaping the Wrath of Bugbear.B



It was a close call but the majority of users on the Kentucky Information Highway escaped infection from the rogue BugBear.B worm that spread rapidly over the Internet in June. Bugbear.B is a variant of the Bugbear worm that wreaked havoc on computers last year. Bugbear.B installs a program on infected machines that collects personal information such as passwords and credit card numbers. It will also disable any anti-virus software that is loaded on your machine and halts personal firewall applications making your PC an open target for hackers.

One reason for the defeat of Bugbear.B may have been the fast reaction by GOT and state agencies to update their virus definition files (aka McAfee DAT files) that provide protection against the worm. GOT received advanced notice of Bugbear.B via a security alert subscription it holds with Symantec. In response, GOT immediately sent out an email to all state agency CIOs and GOT staff warning them of the worm. GOT's LAN/WAN team also installed the McAfee DAT on all GOT email servers, which immediately placed a barrier to Bugbear.B from infiltrating the Commonwealth's Intranet via email.

The moral of this story is that an ounce of prevention is definitely worth a pound of cure, especially in the case of Bugbear.B. By installing the necessary DAT files in a timely manner, network/system administrators helped stave off a major worm outbreak.

For more information on GOT Security Alerts and the importance of applying patches and updates, please see the article on page two of this newsletter: Security Alerts: How They Can Help Protect Your Systems.

Security Alerts: How They Can Help Protect Your Systems

GOT continually strives to keep its staff and customers updated on the latest system security threat information. In an effort to keep abreast of the numerous IT security threats and vulnerabilities that are discovered every day, GOT subscribes to Symantec Corporation's DeepSight Alert Service. DeepSight provides the latest data on hardware and software vulnerabilities, as well as late breaking information on virus, worm, and other malicious code threats.

The alerts are an invaluable resource in protecting the Commonwealth's systems from various security threats by providing information on the latest

hardware and software patches, patch download links, as well as information on detecting and removing malicious code from systems.

Alerts relevant to the Enterprise approved IT products are posted to the Division of Security Services' website at <http://kygovnet.state.ky.us/protected/got/secalert/alerts.htm>.

Network and system administrators are strongly encouraged to bookmark the Security Alerts web page and check it daily. In addition, GOT recommends that agencies devise procedures to ensure the timely installation of

hardware and software patches/updates, as well as the update of virus definition files.

Note: GOT also sends out email notifications for those alerts that are deemed to be a severe security threat. To subscribe, contact Julie Schuller at julie.schuller@mail.state.ky.us. Please note that the current license with Symantec's DeepSight Alert Services prohibits the distribution of alerts to anyone other than GOT staff or its Intranet customers.



“Network & system administrators are strongly encouraged to bookmark the Security Alerts web page and check it daily”

HELP— I Have a Virus!

Sure, we all know the importance of having anti-virus software on our computers. And we also know that it is especially crucial to update our anti-virus software's virus definition files on a regular basis. But do you know the proper GOT procedures to follow if your anti-virus software detects an actual virus, worm or other malicious code on your PC?

The first thing you should do is immediately notify your network support staff that you have a virus on your PC. Do not attempt to remove the virus yourself since your network team will know the correct removal procedures to follow for the particular virus.

Network staff will complete a Security Incident Reporting Form (GOT-F012) to report to the Division of Security Services.

Below are a few virus prevention tips:

- Always have the latest virus definition files & scanning engine installed on your PC.
- Do not open email that comes from an unknown source.
- Never open an attachment that has a double extension such as pictures.jpg.exe.
- Disable AutoPreview in Outlook since this will prevent infected email from automatically being opened.
- Delete chain emails & junk email.



Virus Warning Signs:

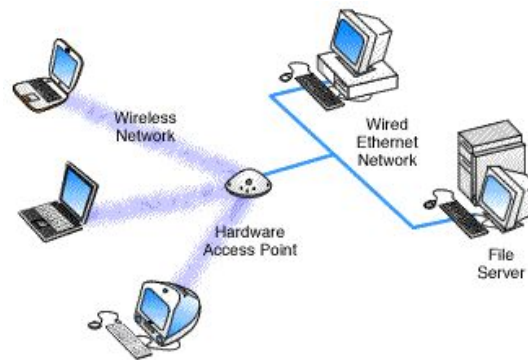
- ◆ Unusual messages or displays appear on your monitor.
- ◆ Unusual sounds or music plays at random times.
- ◆ Your system has less available memory than it should.
- ◆ A disk or volume name has been changed.
- ◆ Unknown program or files have been created.
- ◆ Some of your files become corrupted or don't run properly.

Information for this article was gathered from an article on TechTV.com, Protect Your PC from Viruses, by Shawn Connally & Bruce Stewart.

New Enterprise Wireless LAN Policy

In the last issue of the GOT Security Awareness Newsletter, we featured an article on the security implications of installing wireless LANs. Since that time, the Commonwealth's CIO Office has released an enterprise Intranet Wireless LAN (WLAN) Policy (CIO-078) that is available for review on GOTSOURCE.

In summary, the policy outlines the security & data integrity measures required before implementing any WLAN installation within the Commonwealth's Intranet zone.



The policy states that an agency should not undertake wireless deployment for any operations until it has examined and can acceptably manage and mitigate the risks to its information, system operations, and continuity of essential operations.

In addition, it is recommended that agencies perform a risk assessment and develop a security policy before purchasing wireless technologies because their unique security requirements will determine which products should be considered for purchase.

“An agency should not undertake wireless deployment for any operations until it has examined and can acceptably manage & mitigate the risks”

Using Email Wisely

Did you know that the email communications that you perform daily as you conduct the Commonwealth's business is considered an open record? That means the contents of your email Inbox, if requested, can be made available to the public for review. That is reason enough for everyone to use email wisely in accordance with the enterprise Internet and Electronic Mail Acceptable Use Policy (CIO-060).

The disclosure of business email is more prevalent than you might think. In a survey of 1,100 US companies conducted by PCWorld.com, “14 percent of companies say they have been ordered by a court or regulatory body to produce employee email, and 22 percent of companies report firing an employee for a transgression related to email.” You may want to keep this in mind the next time you draft another email. It may be made public for everyone's eyes.

Some Email DOs & DON'Ts:

- Do maintain a professional tone in your correspondence.
- Do represent yourself and your agency honestly & accurately.
- Do use proper spelling, grammar, & punctuation since this reflects on the Commonwealth's reputation.
- Don't use email for personal business or gain.
- Don't transmit offensive or inappropriate email.
- Don't use abusive or objectionable language.
- Don't forward chain letters or send Spam.
- Don't use email to solicit money for religious or political causes.

Did You Know?

It took the SQL/Slammer Worm that infiltrated the Intranet in January 2003 only 10 minutes to spread worldwide.—Caida.org

Cyber Bytes



Homeland Security

New National Cyber Security Division

In June, the national Department of Homeland Security created a new division to handle cyber security. According to the National Infrastructure Protection Center, "the National Cyber Security Division (NCS D) will provide 24x7 functions, including conducting cyberspace analysis, issuing alerts & warnings, improving information sharing, responding to major incidents, and aiding in national-level recovery efforts."

The NCS D will be comprised of 60 staff whose main mission will be as follows:
—Identify risks & help reduce the vulnerabilities to government's cyber assets and coordinate with the private sector to identify and help protect the America's critical cyber assets.
—Oversee a consolidated Cyber Security Tracking, Analysis, & Response Center (CSTAR C) which will

detect & respond to Internet events, track potential threats & vulnerabilities to cyberspace, and coordinate cyber security and incident response with federal, state, local, private sector, and international partners.
—Create in coordination with other appropriate agencies, cyber security awareness and education programs, and partnerships with consumers, businesses, academia, and international communities.

— NIPC

"The NCS D will provide 24x7 functions, including conducting cyberspace analysis, issuing alerts & warnings... responding to major incidents and aiding in national-level recovery efforts..."

Anti-Spam Products Don't Cut It?

ICSA Labs, which runs one of the most important security industry certifications programs, has recorded disappointing results in its preliminary tests of eight open source and commercial anti-spam packages. Larry Bridwell, program

manager at ICSA Labs, an independent division within TruSecure, said it had "trouble getting up to 60 percent" recognition of spam email in the products it has tested thus far.

— The Register



"ICSA Labs... said it had trouble getting up to 60 percent recognition of spam email in the products it tested thus far."

Malicious Code More Prevalent Than Ever



According to an article in Security Wire Digest, "For the first half of 2003, 3,855 new viruses were released, an increase of 17.5 percent from the first half of 2002."

BugBear, SoBig and Klez-H are the most frequently reported viruses so far this year. It is predicted that this epidemic will only get worse. Remember to keep those virus definition files updated.

—Information gathered from an article by Mathew Schwartz in Security Wire Digest.

Bumpy Ride

A mysterious software fault in the new guidance computer of the Soyuz TMA-1 spacecraft was the cause of a high anxiety off-course landing, NASA sources tell MSNBC.com.

— MSNBC



Microsoft Information

Flaw in Microsoft Windows Media Player

A security issue has been identified in Microsoft Windows Media Player 9 that could allow an attacker to read files or run programs on your computer after you viewed a Web page.



You can help protect your computer by installing an update from Microsoft. Check out the Microsoft Security Bulletin MS03-021 Security Update for Windows Media Player at <http://go.microsoft.com/?linkid=179122>.

Security Update for Microsoft Windows 2000

A security issue has been identified that could allow an attacker to execute commands on a computer running Microsoft Windows(R) 2000. This issue only affects computers running web services. For more information, check out the Microsoft Security Bulletin MS03-022 at http://www.microsoft.com/security/security_bulletins/ms03-022.asp.

Microsoft Issues Windows 2000 Service Pack 4



In late June, Microsoft issued Service Pack 4 for Windows 2000. This Service Pack includes all known security patches and fixes since the operating systems' release. According to Microsoft, Windows 2000 SP4 provides the latest updates in the following areas: security, operating system reliability, application compatibility and setup. This service pack includes fully regression-tested versions of the patches for all security vulnerabilities affecting Windows 2000 found up to the closing date of service pack development. For more information on SP4 for Windows 2000, check out the following Microsoft website: <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/w2ksp4.asp>.

Microsoft Internet Explorer HR Align Buffer Overflow Vulnerability

Microsoft's Internet Explorer is reported to be prone to a buffer overflow in the Align attribute of the HR tag, making it possible for an attacker to cause IE to fail. This vulnerability affects Internet Explorer versions 5 and above. Earlier versions may also be vulnerable.

At this time Microsoft does not have a patch for this vulnerability. To mitigate this threat, it is recommended that all client software be run as a non-privileged user with minimal access rights and the web client should be run as an unprivileged user. Users are also advised not to follow links that originate from a suspicious, untrusted or unfamiliar source.





KENTUCKY GOVERNOR'S OFFICE FOR TECHNOLOGY

Division of Security
Services
101 Cold Harbor Drive
Frankfort, KY 40601

Phone: 502-564-7680
Email: GOTSecurityServices
@mail.state.ky.us

We're on the Web!
ky.gov/got/security/

GOT Security Services — Keeping the Commonwealth's Computing Resources Secure

GOT's Security Awareness Newsletter is published bi-monthly by the Division of Security Services. Its purpose is to provide security and information systems professionals with timely information on cyber vulnerabilities, information security trends, virus information, and security policies and practices.

About the Division of Security Services

The Division of Security Services' (DSS) primary role is to protect and ensure the confidentiality, integrity, and availability of the Commonwealth's computing environment, which includes the Kentucky Information Highway (KIH), Commonwealth Data Center (CDC), and other key state computing facilities.

Security Services is also responsible for the development and maintenance of the GOT Security Policies and Procedures Manual (SPPM), GOT's disaster recovery/business continuity plan, and Security Administrator Manuals (SAMs) that aid network administrators in securely configuring Windows NT, 2000, and Unix Solaris & AIX systems. DSS also provides mainframe RACF, computer forensics, and password auditing services to state agencies upon request. If you would like to learn more about the services that DSS provides, visit our web page at ky.gov/got/security.

For more information on IT Security, check out the following websites!

www.cert.org—The CERT Coordination Center (CERT/CC) is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

www.nai.com—Network Associates aspires to be the worldwide leader in network security and availability for e-business. Founded as McAfee Associates in 1989, Network Associates, Inc. was created by the merger of McAfee Associates and Network General in December of 1997.

www.securityfocus.com—Security Focus ensures the integrity of enterprises' assets through its SIA – Security Intelligence Service. SIA enables IT managers to get the latest vulnerability information as soon as it becomes available through email, voice message, fax, or SMS (Small Message Service) on wireless phones.

www.zdnet.com—ZDNet operates a worldwide network of websites for people who want to buy, use, and learn about technology.